CLAIMS

What is claimed is:

1	1.	A method comprising:
2		comparing at least a subset of information received from a wired network device with
3	inforn	nation previously stored to determine if a rogue access point is present.
1	2.	The method of claim 1, wherein comparing at least a subset of information received from
2	a wire	d network device with information previously stored to determine if a rogue access point is
3	preser	nt comprises:
4		comparing at least a subset of information received in a security report from a legitimate
5	access	s point with information previously stored to determine if a rogue access point is present.
1	3.	The method of claim 1, wherein comparing at least a subset of information received from
2	a wire	d network device with information previously stored to determine if a rogue access point is
3	preser	at comprises:
4		comparing at least a subset of client network traffic received with information previously
5	stored	to determine if a rogue access point is present.
1	4.	The method of claim 1, further comprising:
2		initiating countermeasures against rogue access points determined to be present.
1	5.	The method of claim 4, wherein initiating countermeasures against rogue access points
2	detern	nined to be present comprises:

- 3 denying of service to rogue access points and/or clients connected to rogue access points 4 determined to be present. 6. 1 An electronic appliance, comprising: 2 a network interface to receive information; and 3 a security engine coupled with the network interface, the security engine to compare at 4 least a subset of information received from a wired network device with information previously 5 stored to determine if a rogue access point is present. 1 7. The electronic appliance of claim 6, wherein the security engine to compare at least a 2 subset of information received from a wired network device with information previously stored 3 to determine if a rogue access point is present comprises: 4 the security engine to compare at least a subset of information received in a security 5 report from a legitimate access point with information previously stored to determine if a rogue 6 access point is present. 1 8. The electronic appliance of claim 6, wherein the security engine to compare at least a 2 subset of information received from a wired network device with information previously stored
- 3 to determine if a rogue access point is present comprises:
- 4 the security engine to compare at least a subset of client network traffic received with 5 information previously stored to determine if a rogue access point is present.

- 1 9. The electronic appliance of claim 6, further comprising the security engine to initiate
- 2 countermeasures against rogue access points determined to be present.
- 1 10. The electronic appliance of claim 9, wherein the security engine to initiate
- 2 countermeasures against rogue access points determined to be present comprises:
- 3 the security engine to deny service to rogue access points and/or clients connected to
- 4 rogue access points determined to be present.
- 1 11. A storage medium comprising content which, when executed by an accessing machine,
- 2 causes the machine to implement a security agent in the accessing machine, the security agent to
- 3 compare at least a subset of information received from a wired network device with information
- 4 previously stored to determine if a rogue access point is present.
- 1 12. The storage medium of claim 11, wherein the content to compare at least a subset of
- 2 information received from a wired network device with information previously stored to
- determine if a rogue access point is present comprises content which, when executed by the
- 4 accessing machine, causes the accessing machine to compare at least a subset of information
- 5 received in a security report from a legitimate access point with information previously stored to
- 6 determine if a rogue access point is present.
- 1 13. The storage medium of claim 11, wherein the content to compare at least a subset of
- 2 information received from a wired network device with information previously stored to
- determine if a rogue access point is present comprises content which, when executed by the

- 4 accessing machine, causes the accessing machine to compare at least a subset of client network
- 5 traffic received with information previously stored to determine if a rogue access point is
- 6 present.
- 1 14. The storage medium of claim 11, further comprising content which, when executed by
- 2 the accessing machine, causes the accessing machine to initiate countermeasures against rogue
- 3 access points determined to be present.
- 1 15. The storage medium of claim 14, wherein the content to initiate countermeasures against
- 2 rogue access points determined to be present comprises content which, when executed by the
- 3 accessing machine, causes the accessing machine to deny service to rogue access points and/or
- 4 clients connected to rogue access points determined to be present.
- 1 16. An apparatus comprising:
- 2 a wireless access point configured to generate a security report containing at least a
- 3 subset of information received from other access points.
- 1 17. The apparatus of claim 16, wherein the wireless access point complies with the Institute
- 2 of Electrical and Electronics Engineers, Inc. (IEEE) 802.11 specification.
- 1 18. The apparatus of claim 16, further comprising the wireless access point to transmit the
- 2 security report to a networked device.

- 1 19. The apparatus of claim 16, wherein the security report contains one or more of a media
- 2 access control (MAC) address, a service set identification (SSID), a radio frequency (RF) band, a
- 3 RF channel, and/or a signal strength.